INFORMATION TECHNOLOGY POLICIES

Table of Contents

INFORMATION TECHNOLOGY POLICIES

The Office of Information Technology manages several University policies, standards, and guidelines.

- Access Management
- Cloud Security
- Acceptable Use
- Data Classification
- Incident Response
- Threat and Vulnerability Management

ACCESS MANAGEMENT POLICY

Purpose

The purpose of this policy is to mandate requirements for access management controls across the technological environment at Texila American University, University Support Services, (collectively, the Enterprise). This policy will aid the Enterprise in managing access to its information systems.

Scope

This policy applies to all information systems used throughout the Enterprise, whether managed centrally or in a distributed fashion. This policy applies to all individuals and entities who intend to access the Enterprise's information systems and data, including relevant third-party service providers and hosted/cloud-based systems.

Background

Access to the Enterprise's electronic information resources must be managed in a manner that maintains the confidentiality, integrity, and availability of Enterprise resources, and in a manner that complies with any applicable legal and regulatory requirements.

Definitions

- **Authentication:** The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
- **Authorization:** Access privileges granted to a user, program, or process or the act of granting those privileges
- **Multi-Factor Authentication (MFA):** Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., token generation device); or (iii) something you are (e.g., biometric).
- **Least Privilege:** The principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
- **Privileged Access Management (PAM):** The process of managing and protecting credentials to accounts that have some level of administrative access to devices or systems, including local administrator accounts and superusers.
- **User:** Individual or (system) process, acting on behalf of an individual, authorized to access a system

- **Organization User:** An organizational employee or an individual whom the organization deems to have the equivalent status of an employee, including a contractor, guest researcher, or individual detailed from another organization.
- **Non-Organization User:** A user who is not organizational
- **Privileged User:** A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Policy Statement

Access Management is the process of identifying, tracking, controlling, and managing user access rights to information systems. Any user who requests access to systems, applications, or data, must have their identity authenticated. Additionally, user access should be further restricted following the principle of Least Privilege, and in alignment with any Enterprise defined segregation of duties guidelines.

User account provisioning must include the creation of unique credentials for new users and the disablement and revocation of a terminated user's access privileges upon termination.

Privileged access must only be provided to users as needed. Users with privileged user accounts must also have an organizational user account, which follows the principle of least privilege, and must use this organizational user account for their day-to-day job functions. Privileged user accounts must only be used when elevated privileges are required by the system or application.

Where there is any requirement for shared usage of an account this must be signed off by the IT Security division and the responsible manager and all usage must be audited and traceable to an individual authorized user account.

All remote access to the Enterprise's network must utilize a secure solution, which employs multi-factor authentication, and a secure network encryption protocol.

Multi-Factor Authentication

The Office of Information Technology has taken several steps to protect and monitor our Information Systems. As part of its efforts, the OIT has enabled Multi-Factor Authentication which provides a common method of protection for companies like ours, that utilize and store sensitive, personal, and financial information.

CLOUD SECURITY POLICY

Purpose

This policy describes secure practices for Texila American University's, University Support Services (collectively, Enterprise) use of cloud software and storage services. It also highlights security risks introduced by storing non-public information (data) in the cloud and mandates the protection of data stored by Cloud Service Providers (CSPs) with appropriate technological controls.

Scope

This policy applies to all Enterprise data stored or processed by third-party cloud applications, and to all external cloud services, including cloud-based email and document storage.

Background

The Enterprise outsources certain technological services and data storage to third-party CSPs. IT Leadership must determine what kinds of data are appropriate for storing and sharing via cloud services, and how to protect that non-public information. Data classifications can be found in the Data Classification Policy.

Policy Statement

Governance

IT leadership must approve any deployment or use of cloud-based services for Enterprise systems or data. Enterprise is responsible for ensuring that proper security measures are enforced for any cloud storage service offered to faculty, staff, and students. IT Security must define a process for vetting vendors of cloud platforms. This process must involve an assessment of the security posture of any vendors whose cloud platforms will be housing Enterprise data, and the acquisition of contractual terms and conditions from those vendors to take reasonable steps to maintain control and protection of Enterprise data housed on their platforms. Additionally, the Office of Information Technology (IT) must have administrative access to all cloud applications.

Acceptable Use

All employees, faculty, staff, and students who utilize cloud services for data storage must do so in accordance with this policy and the Acceptable Use Policy. Enterprise data must only be stored in Enterprise approved third-party cloud applications. Additional cloud solutions must be proposed through IT Security.

ACCEPTABLE USE POLICY

Purpose

The purpose of this Acceptable Use Policy is to establish minimum criteria for acceptable use of Texila American University and University Support Services (collectively the Enterprise), Information Systems. This policy also strives to support the Office of Information Technology (IT) in maintaining a safe and welcoming Enterprise environment by defining acceptable forms of Enterprise electronic communications.

Scope

This policy applies to all users across the Enterprise's technological environment and represents the minimum requirements for acceptable Information System use. Individual facilities and business units may require additional security controls, as needed. Users of Enterprise Information Systems include any individual or system with access to Enterprise resources.

Additionally, the Enterprise recognizes that secure and acceptable use of its communication resources is an integral part of its security program. Regulating the use of electronic communications, such as the

internet, email, social media, and telephones, is necessary to provide a safe environment for students, faculty, and staff as well as to protect the Enterprise from reputational loss.

Definitions

- **Authorization:** Access privileges granted to a user, program, or process, or the act of granting those privileges
- **Electronic Communications:** resources owned or managed by the Enterprise, including Enterprise issued email addresses or Enterprise maintained mailing lists. This also applies to any publicly accessible electronic communications involving Enterprise students, faculty, or staff
- **Information System:** A set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information
- **Information System Abuse:** Intentional or reckless misuse, alteration, disruption, or destruction of information processing resources
- **Network:** Any information system implemented with a collection of interconnected components
- **Non-Public Information(or Enterprise Data):** Information of which, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the interest or conduct of Enterprise business, or the privacy to which individuals are entitled
- **Password:** A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization

Roles and Responsibilities

- **Office of Information Technology (IT):** The Office of Information Technology is responsible for maintaining this Acceptable Use Policy and implementing controls to prevent and detect abuse of Enterprise systems and resources.
- **Chief Information Officer**: The head of the IT department is the designated chief information officer and is responsible for setting overall policy regarding Enterprise computers, networks, and information systems use and protection.
- **IT Security:** The IT Security division is responsible for advising IT on what controls and technologies must be used to monitor and detect unacceptable system use, and for performing monitoring and detection of system misuse.
- **IT Leadership:** IT Leadership is responsible for periodically reviewing this policy and for educating the user community about the ethical and secure use of Enterprise information systems.
- **Directors, Supervisors, and Department Head:** Management must ensure that all system users within their area of accountability are aware of the responsibilities defined in this policy and must demonstrate a commitment to secure and acceptable system use.

Policy Statement

Acceptable Use

- Any connection between the Enterprise's network and/or devices and the Internet presents an opportunity for outside adversaries to access Enterprise systems and non-public information. With this in mind, all users must interact with the Internet safely and in compliance with this policy.

- All use of Internet communication methods, including but not limited to E-Mail, social media, and messaging apps, must comply with this policy as well as the Social Media Policy.
- Regarding protection of intellectual property, all individuals will abide by the laws and Enterprise policies to be enforced as defined by the Federal Copyright Act of 1976
- Mass E-Mail
    - Sending e-mail to large groups of recipients at once must be reserved for those situations where another method of contact is not practical
    - For administrators, all general announcements to students, faculty, and staff must be made through Enterprise Communications
    - All bulk e-mail messages from students must be directed through the Dean of Students Office.
    - Any user with approved access to E-Mail mailing lists may access those mailing lists, provided such access is for business or educational purposes.

Unacceptable Use of Enterprise Resources

The following actions are considered an unacceptable use of the Enterprise's Information Systems and/or Electronic Communications. Al Enterprise Users must not:

- Store non-public information on personal devices that are not managed by a mobile device manager.
- Perform any act intentionally or irresponsibly, which may impair the operation of Enterprise Information Systems.
- Make unauthorized alterations of the security or network configuration of any Enterprise Information System.
- Share passwords, PINs, tokens, MFA devices, or other authentication information with anyone, including but not limited to coworkers or administrative staff.
- Solicit passwords, PINs, tokens, or other authentication information from anyone, including but not limited to coworkers or administrative staff.
- Utilize Enterprise systems to gain unauthorized access to remote systems or attempt to circumvent any security protections or authentication systems.
- Users of Enterprise Information Systems must not employ a false identity
- Run or install any piece of software on any Information System, whether intentionally or unintentionally, without prior authorization from IT.
- Use Enterprise Information Systems or Electronic Communications systems for personal financial gain, including but not limited to crypto mining and conducting non-enterprise business.
- Deliberately perform acts that are wasteful of computing resources.
- Use Enterprise Information Systems in a manner that would constitute harassment, invasion of privacy, threat, defamation, or intimidation.
- Users may not initiate or participate in a malicious activity with the intent to cause harm to the Enterprise.
- Users communicating via E-Mail may not forward chain letters, send non-public information such as PII by E-Mail, or use "auto-forward" rules to send E-Mail to a non-Enterprise account.

- Users must not provide false or misleading information to obtain additional access rights or manipulate access rights in any way that violates the Enterprise Access Management Policy.
- Place any of the following types of information or software on any Enterprise information systems:
    - Material that infringes upon the rights of another person or organization including but not limited to copyrights, TM, or IP infringement
    - Abusive, profane, or sexually offensive material
    - Pirated software, destructive software, pornographic materials, libelous statements, or any material which may be injurious to another
    - Advertisements for commercial purposes
    - Threatening, libelous, or offensive messages
- Play any game using Enterprise Information Systems, unless that game is instructional, and has been specifically approved by IT
- Connect to websites related to sex, illegal drugs, criminal skills, hate speech, online gambling, or Peer 2 Peer networks

Policy Disclaimers

- Enterprise Information systems and data stored therein are the property of the Enterprise. The Enterprise reserves the right to limit, restrict, or terminate any user's account and inspect, copy, remove, or otherwise alter any software, data, or file on any Enterprise Information System. The Enterprise also reserves and will exercise, the right to review, audit, intercept, access, and disclose all communications or data on Enterprise Information Systems at any time.
- All users of the Enterprise should be aware of the limitations to their privacy when using Enterprise Information Systems
- The Enterprise will not be liable for any personal data loss resulting from efforts to maintain the privacy and security of Enterprise Information Systems
- The Enterprise views the misuse of information systems as a serious matter and will make no ad-hoc exceptions to this policy. Exceptions to this Acceptable Use Policy must be formally requested, in accordance with the Enterprise Policy Lifecycle and Governance Policy.

Personal Use

The Enterprise is not responsible for any loss or damage incurred by an individual as a result of the individual's personal use of Enterprise electronic communication resources. Individual utilization of Enterprise electronic communications for personal purposes is acceptable, provided the individual's actions do not interfere with their obligations to the Enterprise or incur undue costs to the Enterprise in the form of monetary or reputational loss.

Ignorance of this policy does not excuse violations.

DATA CLASSIFICATION POLICY

Purpose

The purpose of this policy is to define the categorization of data assets at Texila American University, University Support Services (collectively, the Enterprise). This policy describes categories to which all of

the Enterprise non-public information types (data) should be mapped to help the Enterprise protect data consistently and appropriately.

Scope

This policy applies to all Enterprise data. For this policy, this includes electronic data either at rest or in transit. Additionally, this policy applies to any data that is hosted or accessed by third-party service providers.

Definitions

- **Personally Identifiable Information (PII):** Information that can be used to distinguish or trace the identity of an individual (e.g., name, Social Security Number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual. Linked data (such as an individual's name in conjunction with their Social Security Number) can be more sensitive than an individual data point.
- **Protected Health Information (PHI):** Any individually identifiable health information transmitted or maintained in electronic media, or in any other form of medium.
- P**ayment Card Industry Data Security Standard (PCI-DSS**): An information security standard for organizations that handle branded credit cards from the major card schemes
- **Family Educational Rights and Privacy Act of 1974 (FERPA):** A federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA):** United States legislation that provides data privacy and security provisions for safeguarding medical information.

Policy Statement

Data may be classified as follows:

Sensitive: Any data where unauthorized disclosure, alteration, loss, or destruction could result in significant harm to the Enterprise. Data to be classified at this tier mayinclude, but is not limited to, PHI, PII, and any data protected by federal, state or local laws and regulations or industry standards. Data should be classified as critical if loss of that data would:

- Cause personal or institutional financial loss or be a violation of a statute, act, or law
- Constitute a violation of confidentiality agreed to as a condition of possessing, producing or transmitting data
- Require Enterprise to self-report to the government and/or provide public notice if the data is inappropriately accessed
- Cause significant reputational harm to the Enterprise

Confidential: Any data where the unauthorized disclosure, alteration, loss, or destruction would have an adverse impact on the Enterprise's mission, safety, finances, or reputation to a lesser extent than data classified as Sensitive. Data to be classified at this tier may include, but is not limited to:

- Records disclosed to school officials with legitimate educational institutions that do not fall under specific regulations like HIPAA, FERPA, etc
- Unpublished research data
- Unpublished Enterprise financial information that does not fall under GLBA, including strategic plans, real estate plans, or facility development plans

Internal: Any Enterprise intellectual property to which employees, faculty, staff, or students may have authorized access. Internal data includes, but is not limited to:

- Internal communications, such as emails, reports, and other documents
- Research information
- Documents including manuals, technical documents such as system configurations, any standards or procedures developed to guide the Enterprise's decisions, or project plans that are strictly for the use of Enterprise personnel or its constituencies

Public: Any data where the unauthorized disclosure, alteration, loss, or destruction would have little to no adverse impact on the mission, safety, finances, or reputation of the Enterprise. Generally, public information is classified as low risk. Publicly accessible data includes:

- Enterprise financial statements and other reports filed with federal or state governments and available to the public
- Copyrighted materials that are publicly available

INCIDENT RESPONSE POLICY

Purpose

The purpose of the Incident Response Policy is to mandate Incident Response activities within Texila American University and University Support Services (collectively the Enterprise). Incident Response (IR) activities at the Enterprise must be driven by a framework to respond quickly, decisively, and appropriately to an incident.

Scope

This policy applies to any response to an IT security incident that originates from, is directed toward, or otherwise impacts the Enterprise and is different from the University Emergency Action Plan

Definitions

- **Event:** An event is any observable occurrence in an Information System and/or Network. Not all events are adverse events.
- **Adverse Event:** An adverse event is an event that is an exception to the normal operation of Information Systems and/or Networks. Generally, adverse events are events with negative consequences, such as; system crashes, packet floods, unauthorized use of system privileges,

unauthorized access to sensitive data, and execution of malware that destroys data. Not all adverse events become incidents.

- **Incident:** An incident is an adverse event that, as assessed by IT Security staff, violates Enterprise Computing Policies; other Enterprise policies, standards, or code of conduct; or threatens the confidentiality, integrity, or availability of IT Information Systems or Enterprise Data.

Roles and Responsibilities

- **Incident Response Team(IRT):** manages incidents pursuant to the Incident Response Plan. It is the responsibility of the Incident Response Team to detect and respond to any incidents.
- **Incident Response Lead**: A single employee, with one or more designated alternates, should oversee the incident response.
- **Incident Response Coordinator:** Employee who is responsible for assembling all the data pertinent to an incident, communicating with appropriate parties, ensuring that the information is complete, and reporting on incident status both during and after the investigation.
- **Incident Response Handler:** Employees who gather, preserve, and analyze evidence so that an incident can be progressed and brought to conclusion.
- **IT Leadership:** IT Leadership is accountable for policy writing, review, testing, and training of this policy.
- **IT Operations:** IT Staff responsible for administering IT Systems, who can be called upon during an incident to complete various actions.
- **Other Employees:** Can include any or all of the following, depending on the incident: Company Officers/Compliance/Legal/HR

Policy Statement

This plan outlines the most general tasks for Incident Response and will be supplemented by specific internal guidelines and procedures that describe the use of security tools and/or channels of communication. These internal guidelines and procedures are subject to amendment as technology changes. This plan includes the following:

- **Preparation:** Includes the establishment and use of policies, procedures, technology & tools, effective governance, and communications plans, that enable the IRT to assess an event and/or respond to an incident.
- **Detection & Analysis:** Detection is the discovery of an adverse event with security tools or notification by an inside or outside party about a suspected incident. This phase includes the declaration and initial classification of the incident. This phase includes sub-procedures for prioritization, escalation, and communication.

- **Containment, Eradication, & Recovery**
    - **Containment:** Where the affected host or system is identified, isolated, or otherwise mitigated. Most incidents require containment, however, containment strategies can vary based on the type of incident
    - **Eradication:** Eradication may be necessary to eliminate components of the incident.

    - **Recovery:** This consists of restoring systems to normal operation, confirming that systems are functioning normally, and vulnerabilities are remediated to prevent similar incidents.

- **Post-Incident Activity:** Includes the activity in which the incident is reviewed to understand at a minimum, what happened, what went wrong, how well was the response implemented/managed, and areas of improvement.
- **Incident Notification:** When an incident is analyzed and prioritized, the incident response team will notify the appropriate individuals so that all who need to be involved will play their roles. Exact reporting requirements can vary from incident to incident, but parties that are typically notified include the Directory of Security, Corporate Officers, HR, Legal, Compliance, Business Owners, and in some cases external vendors, business partners, law enforcement, regulatory authorities, and affected individuals.
- **Documentation:** Information relevant to the incident is maintained according to Enterprise standards. These can include emails, system data, log data, and investigatory notes.

Testing and Adaptation
The Enterprise must test Incident Response capabilities regularly with measures such as simulations.

The IR Plan must include processes for periodic review and the incorporation of lessons learned after an incident or formal IR testing has occurred. Updates made to the IR Plan must be approved by the Cyber Security Committee and communicated to relevant stakeholders.

THREAT AND VULNERABILITY MANAGEMENT

Purpose
The purpose of this policy is to establish guidance around Texila American University and University Support Services (collectively the Enterprise), Threat and Vulnerability activities. This policy outlines requirements for identification, assessment, and mitigation of threats to the Enterprise's systems, and vulnerabilities within those systems. This document mandates the operational procedures required, including vulnerability scanning and assessment, patch management, and threat intelligence gathering.

Scope
This policy applies to all Information Systems used throughout the Enterprise, whether managed centrally or in a distributed fashion.

Background

The Enterprise is committed to a secure information technology environment in support of its mission and recognizes the need to identify and manage security threats and vulnerabilities. The Enterprise's Risk Management Policy authorizes the Risk Management Team to make informed decisions about managing security risks by gathering risk data from multiple sources. That team relies, in part, on Enterprise's Threat and Vulnerability Management efforts as a source of risk information.

Definitions

- **Threat:** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
- **Vulnerability:** Any weakness in an information system, system procedures, internal controls, or implementation that can be exploited or triggered by a threat source.
- **Vulnerability Scanning:** A technique used to identify devices, device attributes, and associated vulnerabilities.
- **Vulnerability Analysis:** Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.
- **Penetration Testing:** Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network, often involving issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers.
- **Patch Management:** The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions.
- **Threat Intelligence:** The aggregation of knowledge about prominent and emerging security exploits that can be used to inform decisions about how to expand and improve SGU's overall security program.
- **Indicators of Compromise (IOC):** Artifacts that are observed on a network or in an operating system that increases confidence that the network or system has been compromised by a threat actor. These include virus signatures and Internet Protocol (IP) addresses, MD5 message-digest algorithm hashes of malware files or Uniform Resource Locators (URL) or domain names of botnet command and control servers.

Roles and Responsibilities

The Office of Information Technology: The Office of Information Technology (IT) is responsible for vulnerability management efforts, including vulnerability scanning and criticality assessment.

IT Security: IT Security is responsible for threat intelligence gathering efforts, including the monitoring of global services and forums that provide updates on prominent and growing security threats.

Business Owners: Business owners are responsible for understanding and serving as the point of contact for, specific assets within the Enterprise's technological environment.

Policy Statement

Threat Intelligence

Threat intelligence refers to the process of gathering and analyzing information about prevalent or newly discovered attacks or exploits. IT Security must maintain a body of sources for threat intelligence gathering. These sources can include paid services from threat intel providers, or free threat intel forums and communities available on the internet. Gathered threat intelligence should highlight commonly targeted devices and newly discovered Indicators of compromises (IOCs).

Vulnerability Scanning

IT Security will conduct regular vulnerability scans to identify security gaps in the Enterprise's devices and network. These scans will report on any identified vulnerabilities and assign them a generic vulnerability risk score. It's the responsibility of the IT Security team to assess these vulnerabilities and prioritize them based on risk to the Enterprise.

Patch Management

The Enterprise's IT is also responsible for the patching of all systems. Based on the prioritization described above, IT must regularly apply patches to systems with the most critical vulnerabilities to mitigate the threat of exploitation. Information for all applied patches must be tracked, including patch version, patched devices, and the date and time of patching.

Penetration Testing

Penetration testing shall be performed regularly both internally and by a third party, and any additional vulnerabilities identified by penetration testing should be handled by IT as part of vulnerability management.

POLICY FOR PROTECTING PARTICIPANT AND STAFF DATA

Introduction

This policy outlines the commitment of Texila American University (TAU) to protecting the privacy and security of data collected from participants and staff involved in research projects and programs.

Purpose:

This policy establishes guidelines for the ethical and responsible collection, storage, use, and disposal of participant and staff data.

Definitions:

- **Participant:** An individual who voluntarily agrees to participate in a research project or program.
- **Staff:** Employees of TAU involved in research or programs collecting data.
- **Personally Identifiable Information (PII):** Any data that can be used to identify a specific individual (e.g., name, address, date of birth, social security number).
- **De-identified Data:** Data where PII has been removed.
- **Pseudonymized Data:** Data where PII is replaced with a code that can only be linked back to the individual with a separate key.

Informed Consent:

- Informed consent is mandatory before collecting any data from participants.
- Consent forms should be:
    - Written in clear and understandable language.
    - Available in multiple languages if necessary.
    - Explain the type of data collected, the purpose of collection, how it will be used, and who will have access.

- Outline participant rights, including the right to withdraw consent at any time.

Data Minimization:

- Collect only the data necessary to achieve the research or program objectives.
- Avoid collecting sensitive data unless essential for the project and with explicit consent from participants.

Data Security:

- Implement robust security measures to protect data from unauthorized access, disclosure, alteration, or destruction. This includes:
  - Encrypting sensitive data at rest and in transit.
  - Utilizing secure storage systems with access controls (restrict access based on "need to know").
  - Conducting regular security audits and training staff on data security practices.

Data Retention:

- Define a clear data retention policy outlining how long data will be stored based on project needs and legal requirements.
- Establish a secure disposal process for data that is no longer needed.

Data Sharing Agreements:

- If data needs to be shared with third parties, have written agreements outlining:
  - Specific data being shared.
  - Purpose of data sharing
  - Security measures the third party must adhere to
  - Restrictions on data use and further sharing

Staff Training:

- Train staff on data protection practices, including:
  - Participant confidentiality and informed consent procedures
  - Data security measures
  - Proper data collection, storage, and disposal methods

Anonymity and Pseudonymization:

- Whenever possible, anonymize data by removing PII.
- If anonymization is not feasible, use pseudonymization to protect participant identities during data analysis.

Data Breach Notification:

- Develop a plan for responding to data breaches in a timely and transparent manner. This includes:
    - Investigating the breach
    - Notifying affected individuals and relevant authorities (as required by law)
    - Taking steps to mitigate future breaches.

Transparency:

- Be transparent about data collection practices and how participant and staff information will be used.

Review and Update:

- This policy will be reviewed and updated periodically to reflect evolving legal requirements and best practices in data protection.

Contact:

- For any questions or concerns regarding data protection, please contact the IT Department at Jesvin.p@tau.edu.gy

By implementing this policy, Texila American University demonstrates its commitment to protecting the privacy and security of data entrusted to us.